Trivial Nonce-Misusing Attack on Pure OMD

Tomer Ashur and Bart Mennink
February 27, 2015

Dept. Electrical Engineering, ESAT/COSIC, KU Leuven, and iMinds, Belgium
`firstname.lastname@esat.kuleuven.be`

Abstract. Pure OMD is an authenticated encryption mode that will be presented by Reyhanitabar et al. at FSE 2015. It is (among others) claimed to achieve authenticity against nonce-misusing adversaries. We show that this claim is incorrect, by presenting an adversary that makes 3 queries (including the forgery) of a total complexity 6.

1 Introduction

Offset Merkle-Damgård (OMD) is a submission to the CAESAR competition [1] by Cogliani et al. [2]. It is characterized by the usage of a full-fledged compression function, and in fact the CAESAR submission takes the sha256 compression function. OMD is proven to achieve birthday-bound security on the state against adversaries that are not allowed to re-use the nonce. At ProvSec 2014, Reyhanitabar et al. [3] showed how to generalize the scheme to achieve security against nonce-misusing adversaries. On the downside, these schemes are not online and are less efficient than OMD. At FSE 2015 Reyhanitabar et al. [4] will present pOMD (pure OMD). pOMD improves over classical OMD in that the associated data is processed almost for free. The authors prove that pOMD inherits all security features of OMD, particularly birthday-bound security against nonce-respecting adversaries. As a bonus, the authors claim authenticity against nonce-misusing adversaries.

Our Contribution

We show that pOMD *does not* achieve authenticity against misuse-resistant adversaries. In fact, we show an attack on pOMD that makes three evaluations (including the forgery) of total complexity 6 primitive calls and succeeds with probability 1.

We remark that the attack is specific for pOMD and relies on the right of the adversary to misuse the nonce. Consequently, the attack does *not* invalidate the main result of pOMD on nonce-respecting adversaries. It additionally does *not* apply to the OMD CAESAR submission and to the misuse-resistant variants of [3].

2 pOMD

Let $k, m, n, \tau \in \mathbb{N}$ such that $m \leq n$. Let $F : \{0,1\}^k \times \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^n$ be a keyed compression function. pOMD is a mapping that takes as input a key $K \in \{0,1\}^k$, a nonce $N \in \{0,1\}^{\leq n-1}$, an arbitrarily sized associated data $A \in \{0,1\}^*$, and an arbitrarily sized message $M \in \{0,1\}^*$, and it returns a ciphertext $C \in \{0,1\}^{|M|}$ and tag $T \in \{0,1\}^\tau$.

For our attack it suffices to describe pOMD for the specific case where $|A| = 2n$ and $|M| = m$ (or in other words, the associated data consists of two integral blocks and the

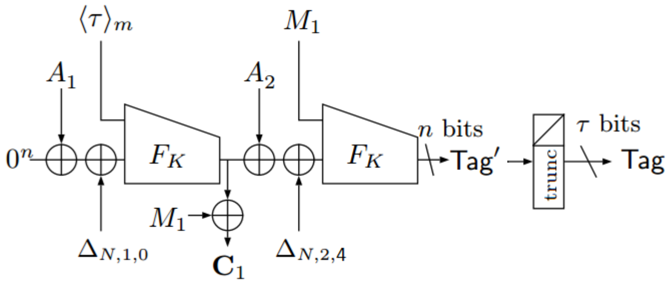

Fig. 1: pOMD for the specific case of $|A| = 2n$ and $|M| = m$.

message of one integral block). It is depicted in Fig. 1 (and corresponds to Case A of [4]). Here,

$$\begin{aligned}\varDelta_{N,1,0} &= F_K(N\|10^{n-1-|N|}, 0^m) \oplus 16F_K(0^n, 0^m)\,,\\ \varDelta_{N,2,4} &= F_K(N\|10^{n-1-|N|}, 0^m) \oplus (32 \oplus 16 \oplus 4)F_K(0^n, 0^m)\,,\end{aligned}$$

but our attack will not effectively use these masking values.

3 Security of pOMD

Security of an authenticated encryption scheme $\varPi = (\mathcal{E}, \mathcal{D})$ is usually measured using privacy and authenticity. For privacy, we consider an adversary that tries to distinguish $\mathcal{E}_K$ for uniformly random $K \xleftarrow{\$} \{0,1\}^k$ from an ideal encryption scheme \$ with the same interface. For integrity, we consider an adversary that tries to forge a ciphertext, which means that $\mathcal{D}_K$ ever returns a valid message (other than $\perp$) on input of (N, A, C, T) and no previous encryption query $\mathcal{E}_K(N, A, M)$ returned (C, T).

In these games, the adversary is limited in a certain sense. In more detail, we consider two types of adversaries: *nonce-respecting*, where no two encryption queries should be made with the same nonce, and *nonce-misusing*, where multiple encryption queries with the same nonce are allowed.

Security Claim of pOMD

Assuming that F underlying pOMD is sufficiently secure (as we assume sha256 to be), Reyhanitabar et al. [4] prove the following security levels:

	privacy	authenticity
nonce-respecting	$2^{n/2}$	$2^{n/2}$
nonce-misusing	0	$2^{n/4}$

We refer to [4] for the technicalities regarding the bounds.

4 Nonce-Misusing Attack on pOMD

We consider a nonce-misusing adversary that operates as follows:

(i) Fix $N = \varepsilon$ and choose arbitrary $M \in \{0,1\}^m$ and $A_1, A_2, A_1' \in \{0,1\}^n$ such that $A_1 \neq A_1'$;

(ii) Query $\text{pOMD}_K(N, A_1A_2, M) \to (C, T)$;
(iii) Query $\text{pOMD}_K(N, A_1'A_2, M) \to (C', T')$;
(iv) Set $A_2' = C \oplus C' \oplus A_2$;
(v) Query forgery $\text{pOMD}_K^{-1}(N, A_1'A_2', C', T)$.

For the first and second evaluation of pOMD, it holds that the state difference right *before* the second F-evaluation equals $C \oplus C'$. The forgery is formed simply by adding this value to A_2. Consequently, it holds that the first call to pOMD and the forgery attempt have the exact same input to the second F-evaluation, and thus the same tag. Therefore, the forgery attempt succeeds as

$$\text{pOMD}_K^{-1}(N, A_1'A_2', C', T) = M$$

by construction

Where is the Flaw in the Proof

Reyhanitabar et al. [4] claim that pOMD achieves birthday-bound authenticity even against nonce-misusing adversaries, and our attack shows the existence of a flaw in their reasoning. To be precise, the flaw is located in Lemma 4 case 4, and more specifically the analysis of probability $\mathbf{Pr}(\mathsf{intcol} \mid \mathsf{E}_4)$. The authors claim that an adversary can, indeed, find an internal collision, but that any such collision happens with a birthday bound only. This reasoning, however, assumes that the input to every F-call is random, which is not the case given that the adversary can re-use the nonce and thus observe and modify the state using encryption queries.

Acknowledgments. The authors thank Elena Andreeva, Atul Luykx, and Reza Reyhanitabar for their feedback on this note. This work was supported in part by the Research Fund KU Leuven, OT/13/071, and in part by the Research Council KU Leuven: GOA TENSE (GOA/11/007). Bart Mennink is a Postdoctoral Fellow of the Research Foundation – Flanders (FWO).

References

[1] CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness (May 2014), `http://competitions.cr.yp.to/caesar.html`

[2] Cogliani, S., Maimut, D., Naccache, D., do Canto, R.P., Reyhanitabar, R., Vaudenay, S., Vizár, D.: OMD: a compression function mode of operation for authenticated encryption. In: Selected Areas in Cryptography 2014. Lecture Notes in Computer Science, vol. 8781, pp. 112–128. Springer, Heidelberg (2014)

[3] Reyhanitabar, R., Vaudenay, S., Vizár, D.: Misuse-resistant variants of the OMD authenticated encryption mode. In: Provable Security 2014. Lecture Notes in Computer Science, vol. 8782, pp. 55–70. Springer, Heidelberg (2014)

[4] Reyhanitabar, R., Vaudenay, S., Vizár, D.: Boosting OMD for almost free authentication of associated data. In: Fast Software Encryption 2015. Lecture Notes in Computer Science, Springer, Heidelberg (2015), preproceedings version